Splunk - Upgrade Strategy

This document outlines the general strategy to upgrade Splunk Enterprise on-premise.

General Guide

Confirm compatibility

1. Confirm ITSI compatibility. Historically ITSI has been compatible with a wide range of Splunk Enterprise versions, so this has been upgraded first.
2. Confirm add-on and app compatibility. Historically this presents minor to no issues, except for upgrading to version 8 and Python 3, and have been upgraded as needed before or after Splunk Enterprise.

Perform upgrades

1. Upgrade add-ons and apps that are compatible with old & new versions
2. Upgrade ITSI
3. Upgrade Splunk Enterprise following the order as specified in vendor documentation. Be sure to
    a. search heads (be mindful if KVStore updates are needed, such as 8.1 updating the storage engine.
    b. indexers (be sure to update the tsidxWritingLevel in cluster master _cluster/local/indexes.conf [default] stanza to the latest version
    c. forwarders
4. Upgrade add-ons and apps that need to be updated after Splunk enterprise.

Currently, the upgrade installer is copied to each host and run manually. Future improvements would be to automate via Ansible/Tower.

7.2 to 8.1 Specific Steps:

RHEL Install Prep & Commands:

1. Copy installer .tgz to /tmp
2. Change ownership of the file to Splunk: sudo chown splunk:splunk <filename>
3. sudo systemctl stop Splunkd
4. Sudo as Splunk: sudo su - splunk
5. tar -xvzf /tmp/<filename> -C /apps/
6. revert to smomoneng account: exit
7. cd /apps/splunk/bin
8. sudo is needed to update the systemctl configuration: sudo ./splunk start --accept-license --answer-yes

Win Install Prep & Commands:

1. Copy installer .msi to D:\temp
2. Open cmd as admin
3. D:
4. cd splunk\bin
5. splunk stop
6. cd D:\temp
7. <filename.msi>
8. Continue through installer UI prompts

Note: All hosts can have the app all_date_patch_props (or idxc_date_patch_props for IDX cluster members) removed as this patched a date/time flaw in older versions of Splunk Enterprise.

Search Head Cluster:

1. Update Deployer but do not restart, leave stopped
2. Upgrade each SHC member to 8.1 one at a time
3. **On ITSI SHC members,** remove /apps/splunk/etc/apps/SA-ITOA/local/limits.conf which contains the stanza [search] phased_execution_mode=auto. This is not needed on newer versions of Splunk Enterprise.
4. **On Core SHC members,** in /etc/apps/splunk_secure_gateway create /local/app.conf with the stanza:
   [install]
   state = enabled
5. Remove all_date_patch_props from deployer /etc/apps/
6. Remove all_date_patch_props from deployer /etc/shcluster/apps/
7. Start Deployer
8. Prepare each SHC member for the KVStore update one at a time:
    a. Add the following stanza to /etc/system/local/server.conf:
       ```
       [kvstore]
       storageEngineMigration=true
       ```

    b. Restart Splunk on the search head cluster member
    c. **From your personal laptop** open cmd as admin and run the following command:

```
curl -k -u admin:<password> https://<server name>:8089/services/shcluster/captain/kvmigrate/start -d
storageEngine=wiredTiger -d isDryRun=true
```

    d. Confirm ready for update is True
9. **On the SHC captain** sudo to Splunk ID and execute the following command:

```
./splunk start-shcluster-migration kvstore -storageEngine wiredTiger
```

10. Execute the following command periodically to check progress of kvstore:
```
./splunk show shcluster-kvmigration-status
```

11. Execute the following command to confirm kvstore status:
```
./splunk show kvstore-status
```

12. After completion, update add-ons that were not backward compatible with version 7
13. Update CL_SHC app to add role securegateway to all users and push SHC bundle
14. Copy Cloud Gateway config to Secure Gateway (reference https://docs.splunk.com/Documentation/SecureGateway/2.0.1000/Admin/Transition#Copy_data_from_Splunk_Cloud_Gateway_to_Splunk_Secure_Gateway)
15. Remove deprecated role cloudgateway from CL_SHC/local;authorize.conf; remove SHCluster app splunk_app_cloudgateway and push SHC bundle

Indexer Cluster:

1. Upgrade master node to 8.1
2. Remove all_date_patch_props app from master node and restart Splunk
3. Upgrade each IDX cluster member to 8.1 one at a time
4. Add the following stanza to the top of master _cluster/local/indexes.conf:
```
[default]
tsidxWritingLevel=4
```

5. Remove idxc_date_patch_props from master-apps
6. Validate and push cluster bundle to apply tsidx update
7. Validate health of IDX cluster

Forwarders:

Note: SSSHFAPP3 WILL NOT BE UPDATED AS PART OF THIS CHANGE. TA-db-monitor is not Python3 compatible. 7.x forwarders are compatible with 8.x indexers, so in a future change we will do one of 3 things:

- Upgrade ssshfapp3 to a newer version of 7
- Upgrade ssshfapp3 to 8 and keep Python2 as default interpreter
- Determine if TA-db-monitor can be converted to run on Python3 and upgrade to 8

For all other forwarders:

1. Update 1 at a time
2. Remove all_date_patch_props app and restart Splunk
3. Update post-upgrade add-ons that were not backward compatible with version 7

Upgrade TAs/APPs that were not backward-compatible with verison 7, as documented at

~~HMSI-423~~ - Splunk 8 Upgrade Readiness Assessment DONE .

Indexer

SHC

Deployment Apps: UFs and HFs

ITSI/SAI (documentation is at https://docs.splunk.com/Documentation/ITSI/4.7.0/Install/UpgradeSHC):

Upgrade SHC:

1. Disable rules engine (searches/reports/alerts itsi_event_grouping)
2. Update SHC
    a. On deployer, update splunk_app_infrastructure/bin/em_model_entity.py line 67 from self.title = title to self.title = lower(title)
    b. Deploy SHC bundle
    c. Login to SHC
    d. Load ITSI and walk through upgrade/kvstore migration
3. Re-enable rules engine

Upgrade indexers:

1. Make a backup of Splunk_TA_Infrastructure/local/props.conf and /transforms.conf
2. Copy SA-IndexCreation and Splunk_TA_Infrastructure to cluster master /etc/master-apps
3. Ensure props and transforms from step 1 are included
4. Deploy cluster bundle

Update HF:

1. On Deployment Server, update HF_Splunk_TA_Infrastructure
2. Ensure local/props.conf is included
3. Deploy

Update License Server:

1. Copy SA-ITSI-Licensechecker and SA-UserAccess
2. Restart Splunk

Validate upgrade

Splunk minor versions are supported for two years from release. General recommendation is to upgrade Splunk Enterprise every 12 months to a major version after release (typically Octoboer), with incremental minor upgrades only if necessary to remediate issues. ITSI can be upgraded at any time as upgrades are more rapid with iterative improvements.

Vendor general documentation is at https://docs.splunk.com/Documentation/Splunk/latest/Installation/HowtoupgradeSplunk.

Distributed upgrade order is at https://docs.splunk.com/Documentation/Splunk/latest/Installation/UpgradeyourdistributedSplunkEnterpriseenvironment.

Related articles

- Splunk - TA-NIX Customization
- Splunk - Dell EMC Monitoring - PMX Storage Array Setup
- Splunk - Enterprise Installation Instructions
- Splunk - DB Server On-boarding
- Splunk - Circuit Breaker Triage Steps